Fundamentals of Cryptography: Problem Set 8

Due Wednesday Dec 3, 3PM

Collaboration is permitted (and encouraged); however, you must write up your own solutions and acknowledge your collaborators.

If a problem has **0pt**, it will not be graded.

Problem 0 Read section Digital Signature Schemes of Katz & Lindell, or section Digital Signatures and Fast hash-based signatures of Boneh & Shoup, or lecture 11, 12, 13 of course 6.875 in `mit6875.org`.

Problem 1 (5pt, Exercise 13.4 from BS) DSKS attack on RSA Let us show that the RSA-based signature scheme is vulnerable to the duplicated signature key selection (DSKS) attack. You task is to construct a p.p.t. adversary $\mathcal{A}$ winning the following game with good probability:

- The adversary is given the public key $pk = (n, e)$, and chooses a message m.
- The adversary is given the signature σ satisfying $\sigma^e = H(m)$, and outputs a public key $pk' = (n', e')$ and its corresponding secret key $sk' = d'$.
- The adversary wins if 1) $\mathsf{Verify}(pk', m, \sigma) = 1$ and 2) (pk', sk') is a valid key pair, i.e., n' is the product of two λ-bit primes, $e'd' \equiv 1 \mod \phi(n')$.

Hint: There is a hint in the textbook of Boneh & Shoup.

Problem 2 (6pt) Signature based on Preimage Sampleable Functions As mentioned in the class, digital signature can be constructed from any trapdoor one-way permutation in the random oracle model. In this problem, we replace trapdoor one-way permutation with preimage sampleable functions (PSF).

Definition 1. *Preimage Sampleable Functions (PSF)* consists of a few p.p.t. algorithms

- $\mathsf{TrapGen}(1^n)$ samples (a, t), where a is the description of an efficiently-computable function $f_a : \mathcal{D}_n \to \mathcal{R}_n$ (domain $\mathcal{D}_n$ and range $\mathcal{R}_n$ are efficiently recognizable and are determined by the security parameter n) and t is the trapdoor of f_a.
- $\mathsf{SampleDom}(1^n)$ samples x from some distribution over $\mathcal{D}_n$.
- $\mathsf{SampleRan}(1^n)$ samples y uniformly from $\mathcal{R}_n$.
- $\mathsf{SamplePre}(t, y)$ samples $x \in f_a^{-1}(y)$ from the proper conditional distribution.

such that the following two distributions are identical for any (a, t) sampled by $\mathsf{TrapGen}(1^n)$

$$\left\{ (x, y) : \begin{matrix} x \leftarrow \mathsf{SampleDom}(1^n) \\ y = f_a(x) \end{matrix} \right\} \qquad \left\{ (x, y) : \begin{matrix} y \leftarrow \mathsf{SampleRan}(1^n) \\ x \leftarrow \mathsf{SamplePre}(t, y) \end{matrix} \right\} \tag{*}$$

Part A. PSF also satisfies the following security property:

- **One-wayness without trapdoor:** For any p.p.t. adversary $\mathcal{A}$,

$$\Pr\left[\mathcal{A}\left(1^n, a, y\right) \in f_a^{-1}(y) \middle| \begin{aligned}(a,t) &\leftarrow \mathsf{TrapGen}(1^n)\\ y &\leftarrow \mathsf{SampleRan}(1^n)\end{aligned}\right] \leq \mathrm{negl}(n).$$

Construct a secure digital signature scheme by instantiating the hash-and-sign paradigm with PSFs. You should present the signature scheme and prove it is existentially unforgeable under a chosen-message attack. In your security proof, the hash function $H_n : \{0,1\}^* \to \mathcal{R}_n$ can be modeled as a random oracle.

Part B. Some PSFs (e.g., the next problem) satisfy a stronger property:

- **Collision resistance without trapdoor** For any p.p.t. adversary $\mathcal{A}$,

$$\Pr\left[x \neq x' \wedge f_a(x) = f_a(x') \middle| \begin{aligned}(a,t) &\leftarrow \mathsf{TrapGen}(1^n)\\ x, x' &\leftarrow \mathcal{A}(1^n, a)\end{aligned}\right] \leq \mathrm{negl}(n).$$

Prove that your construction in Part A is strongly existentially unforgeable[1] under a chosen-message attack.

Problem 3 (6pt) Signature based on SIS We have discussed PKE scheme based on the lattice assumption of LWE (Learning With Errors). In this problem, we construct a signature scheme based on another lattice assumption of SIS (Small Integer Solution). Following the previous problem, it suffices to construct PSFs.

Definition 2. The small integer solution problem SIS (in the ℓ_2 norm) is as follows: given an integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and a real β, find a nonzero integer vector $\mathbf{e} \in \mathbb{Z}^m$ such that $\mathbf{Ae} = \mathbf{0} \bmod q$ and $\|\mathbf{e}\|_2 \leq \beta$.

For functions $q(n), m(n)$, and $\beta(n)$, $\mathsf{SIS}_{q,m,\beta}$ is the ensemble over instances $(q(n), \mathbf{A}, \beta(n))$ where $\mathbf{A} \in \mathbb{Z}_q^{n \times m(n)}$ is uniformly random.

SIS problem is find a short vector in the solution space

$$\Lambda^{\perp}(\mathbf{A}) := \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{Ae} = \mathbf{0} \bmod q\}.$$

Note that the solution space $\Lambda^{\perp}(\mathbf{A})$ is a subgroup of $\mathbb{Z}^m$, thus it is a lattice. A lattice can also be represented by its basis

$$\Lambda(\mathbf{B}) := \{\mathbf{Bc} : \mathbf{c} \in \mathbb{Z}^m\},$$

where the column vectors of $\mathbf{B}$ are the basis.

The construction of this problem relies on the following facts:

- $\mathsf{SIS}_{q,m,\beta}$ is believed to be hard for a wide range of parameters when $m, \beta = \mathrm{poly}(n)$, $m \geq n + \Omega(n)$, and prime $q \geq \beta \cdot \omega(\sqrt{n \log n})$.

[1] Strong unforgeability means the adversary will win if it generates a new valid signature for a queried message.

- For any prime $q = \text{poly}(n)$ and $m \geq 5n \log q$, there is a p.p.t. algorithm [Ajtai '99] that samples a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a basis $\mathbf{B} \in \mathbb{Z}^{m\times m}$ (i.e., $\Lambda^\perp(\mathbf{A}) = \Lambda(\mathbf{B})$) such that the distribution of $\mathbf{A}$ is statistically close to uniform over $\mathbb{Z}_q^{n\times m}$ and the "length" $\|\tilde{\mathbf{B}}\| \leq L = m^{2.5}$.

  If you are curious, the length of a basis is defined as follows: Let $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_m \in \mathbb{R}^m$ be the Gram-Schmidt orthogonalization of $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$. That is, $\tilde{\mathbf{b}}_1 = \mathbf{b}_1$ and $\tilde{\mathbf{b}}_i$ is the component of $\mathbf{b}_i$ orthogonal to $\text{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})$. The length of the basis is $\|\tilde{\mathbf{B}}\| = \max_i \|\tilde{\mathbf{b}}_i\|$.

- Given a lattice Λ, a center $\mathbf{c}$, and a Gaussian parameter s, the discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$ over Λ is defined as

  $$D_{\Lambda,s,\mathbf{c}}(\mathbf{x}) \propto \exp\Big(-\frac{\pi\|\mathbf{x}-\mathbf{c}\|_2^2}{s^2}\Big).$$

  There is a p.p.t. algorithm [Gentry-Peikert-Vaikuntanathan '08] that, given a basis $\mathbf{B}$, and $s, \mathbf{c}$, samples from $D_{\Lambda(\mathbf{B}),s,\mathbf{c}}$ as long as $s \geq \omega(\log m) \cdot \|\tilde{\mathbf{B}}\|$.

Construct PSFs based on the hardness of SIS. The function and its trapdoor are sampled by [Ajtai '99]. The function is $f_{\mathbf{A}}(\mathbf{e}) = \mathbf{A}\mathbf{e} \mod q$, whose domain and range are $\mathcal{D} = \{\mathbf{e} \in \mathbb{Z}^m : \|\mathbf{e}\|_2 \leq s\sqrt{m}\}$ and $\mathcal{R}_n = \mathbb{Z}_q^n$. The recommended parameters are $q = \text{poly}(n)$, $m = 5n\log q = \Theta(n \log n)$, $L = m^{2.5}$, $s = L\log^2 n \geq L \cdot \omega(\log m)$. The construction and the proof can be split into the following parts:

Part A. State the domain sampling algoirthm $\mathsf{SampleDom}$ and preimage sampling algorithm using the sampler from [Gentry-Peikert-Vaikuntanathan '08]. Show the two distributions in (*) are statistically close. (This relaxed property also implies digital signature.)

You may need the following properties of discrete Gaussian distribution, under the current parameters: If a lattice has a basis $\mathbf{B} \in \mathbb{Z}^{m\times m}$ satisfying $\|\tilde{\mathbf{B}}\| \leq L$ and for any $\mathbf{c} \in \mathbb{R}^m$, the min-entropy of $D_{\Lambda,s,\mathbf{c}}$ is at least m bits, and

$$\Pr_{\mathbf{x}\leftarrow D_{\Lambda,s,\mathbf{c}}}[\|\mathbf{x}-\mathbf{c}\|_2 > s\sqrt{m}] \leq 2^{-m}.$$

Part B. Prove the one-wayness and collision-resistance of the constructed PSFs, assuming $\mathsf{SIS}_{q,m,2s\sqrt{m}}$ is hard.